UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/501,332	02/09/2000	Charles Merriam	5437-055	3704

22835 7590 07/14/2004

PARK, VAUGHAN & FLEMING LLP
508 SECOND STREET
SUITE 201
DAVIS, CA 95616

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	15

DATE MAILED: 07/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/501,332	MERRIAM, CHARLES	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-33 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-33 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-33 have been re-examined and are the rejected under 35 U.S.C. 102(e).

2. Claims 1, 12, and 23 are rejected under 35 U.S.C. 112, 1st paragraph.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1-33 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 1, 12, and 23 states the "set of information is not available within the system" wherein if Applicant meant the information is completely and/or permanently removed or deleted from the system making the set of information unavailable within the system constitutes new subject material. Specification, on page 10, discusses purging the set of information wherein making the information unrenderable to the user. Specification states that "it is not necessary to delete an information set from a system in order to purge it" (lines

11-13) and also states "that it is effectively purged from the system even if it remains physically within the system" (lines 15-16). Hence, the information sets are still within the system but just unrenderable to the user. Therefore, the "information is not available within the system" is considered newly added matter that was neither discussed previously nor originally discloses in the specification.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

3. Claims 1-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Boneh, Et Al. (US 6,134,660).

As per claim 1:

Boneh, Et Al. teaches a method for managing information retention system (col.5, lines 63-67) wherein includes a central file server 102 having a number of files of electronic information and encrypts the key file before the key file is transferred to the backup system (col.4, lines 17-21).

Boneh discloses the server system receiving a set of information and associating one or more keys with the set of information wherein encrypting the set of information using one or more keys (col.4, lines 53-55). Boneh discusses the set of information is encrypted and storing it in the information system in the form of a backup system (col.4, lines 50-53) and the backup system provides persistent storage for only encrypted information wherein it is inherent the backup system only stores the encrypted information since the information needed to be encrypted before transferring the file to the backup system (col.4, lines 38-42). Hence, the unencrypted set of information is not persistently stored in the backup system.

In addition, Boneh discloses purging the set of information from the system by deleting the key once the key's lifetime is expired or considered as old keys thereby making the set of information inaccessible or unrenderable to a user (col.5, lines 13-22). To purge is to eliminate and to render to produce an image from the data file so unrenderable is to unable to produce the image from the data file. The information set disclosed in Boneh that is associated to the key is unable to be produced or accessed from the system once the key of

that particular file is deleted (col.4, line 65 thru col.5, line 12). Thus, the set of information is inherently no longer available within the system once the key to that particular information set is deleted.

As per claim 2:

Boneh teaches the set of information is purged from the system without requiring that the encrypted form of the set of information be deleted from the one or more repositories (col.5, lines 1-32).

As per claim 3:

Boneh discloses the set of information is stored in the one or more repositories only in encrypted form (col.4, lines 50-55).

As per claim 4:

Boneh includes the keys comprises a symmetrically paired set of keys (col.7, lines 45-62).

As per claim 5:

Boneh discloses receiving a request from an information sink to render the set of information to a user prior to deletion of one or more keys (col.6, lines 26-50). The information sink is inherently a device that receives information from another device. Boneh teaches an information sink involving a network server such as the Internet server and a computer system for communicating information over a network (col.7, lines 28-62).

Boneh further discusses accessing the encrypted set of information from one or more of the repositories, decrypting the encrypted set of information

using a key to derive the set of information (col.7, lines 49-51) and enabling the information sink to render the set of information to the user (col.7, lines 28-62).

As per claim 6:

Boneh discloses the set of information is stored in the one or more repositories only in encrypted form (col.4, lines 50-55) and the encrypted information set is decrypted only when it is necessary to render the set of information to the user (col.8, lines 18-28).

As per claim 7:

Boneh discloses receiving a request from an information sink to render the set of information to a user prior to deletion of one or more keys (col.6, lines 26-50). The information sink is a device that receives information from another device. Boneh teaches an information sink involving a network server such as the Internet server and a computer system for communicating information over a network (col.7, lines 28-62). Boneh further discusses accessing the encrypted set of information from one or more of the repositories, accessing one or more keys (col.4, lines 50-55), and providing the encrypted information and key(s) to enable the information sink to decrypt the encrypted set of information using the key(s) to render the set of information to the user (col.7, lines 28-62).

As per claim 8:

Boneh discloses the set of information is stored in the one or more repositories only in encrypted form (col.4, lines 50-55) and the encrypted information set is decrypted only when it is necessary to render the set of information to the user (col.8, lines 18-28).

As per claim 9:

Boneh discloses determining the method of purging based upon an information retention policy (col.5, lines 25-31), whether the set of information should be purged from the system and should the information set determined to be purged wherein Boneh teaches purging the set of information by deleting the key(s) (col.6, lines 13-15). Thus, making the set of information unrenderable (col.6, lines 13-15).

As per claim 10:

Boneh discusses the information retention policy is time-based such that the set of information is purged after a certain period of time (col.5, lines 13-30).

As per claim 11:

Boneh discusses the retention policy is time-based such that the set of information is purged when one or more conditions are satisfied (col.6, lines 6-15).

As per claim 12:

Boneh, Et Al. teaches a method for managing information retention system (col.5, lines 63-67) wherein includes a central file server 102 having a

number of files of electronic information and encrypts the key file before the key file is transferred to the backup system (col.4, lines 17-21).

Boneh discloses the server system receiving a set of information and associating one or more keys with the set of information wherein encrypting the set of information using one or more keys (col.4, lines 53-55). Boneh discusses the set of information is encrypted and storing it in the information system in the form of a backup system (col.4, lines 50-53) and the backup system provides persistent storage for only encrypted information wherein it is inherent the backup system only stores the encrypted information since the information needed to be encrypted before transferring the file to the backup system (col.4, lines 38-42). Hence, the unencrypted set of information is not persistently stored in the backup system.

In addition, Boneh discloses purging the set of information from the system by deleting the key once the key's lifetime is expired or considered as old keys (col.5, lines 13-22), thereby making the set of information inaccessible or unrenderable to a user (col.4, line 65 thru col.5, line 12). To purge is to eliminate and to render to produce an image from the data file so unrenderable is to unable to produce the image from the data file. The information set disclosed in Boneh that is associated to the key is unable to be produced or accessed from the system once the key of that particular file is deleted. Thus, the set of information is inherently no longer available within the system once the key to that particular information set is deleted.

As per claim 13:

Boneh teaches the set of information is purged from the system without requiring that the encrypted form of the set of information be deleted from the one or more repositories (col.5, lines 1-32).

As per claim 14:

Boneh discloses the set of information is stored in the one or more repositories only in encrypted form (col.4, lines 50-55).

As per claim 15:

Boneh includes the keys comprises a symmetrically paired set of keys (col.7, lines 45-62).

As per claim 16:

Boneh discloses the mechanism of receiving a request from an information sink to render the set of information to a user prior to deletion of one or more keys (col.6, lines 26-50). The information sink is a device that receives information from another device. Boneh teaches an information sink involving a network server such as the Internet server and a computer system for communicating information over a network (col.7, lines 28-62). Boneh further discusses the mechanisms for accessing the encrypted set of information from one or more of the repositories, decrypting the encrypted set of information using a key to derive the set of information (col.7, lines 49-51), and enabling the information sink to render the set of information to the user (col.7, lines 28-62).

As per claim 17:

Boneh discloses the set of information is stored in the one or more repositories only in encrypted form (col.4, lines 50-55) and the encrypted information set is decrypted only when it is necessary to render the set of information to the user (col.8, lines 18-28).

As per claim 18:

Boneh discloses the mechanism for receiving a request from an information sink to render the set of information to a user prior to deletion of one or more keys (col.6, lines 26-50). The information sink is inherently a device that receives information from another device. Boneh teaches an information sink involving a network server such as the Internet server and a computer system for communicating information over a network (col.7, lines 28-62). Boneh further discusses the mechanisms of accessing the encrypted set of information from one or more of the repositories, accessing one or more keys (col.4, lines 50-55), and providing the encrypted information and key(s) to enable the information sink to decrypt the encrypted set of information using the key(s) to render the set of information to the user (col.7, lines 28-62).

As per claim 19:

Boneh discloses the set of information is stored in the one or more repositories only in encrypted form (col.4, lines 50-55) and the encrypted information set is decrypted only when it is necessary to render the set of information to the user (col.8, lines 18-28).

As per claim 20:

Boneh discloses the mechanism for determining to purge based upon an information retention policy (col.5, lines 25-31), whether the set of information should be purged from the system and should the information set determined to be purged wherein Boneh teaches the mechanism for purging the set of information is by deleting the key(s) (col.6, lines 13-15). Thus, making the set of information unrenderable (col.6, lines 13-15).

As per claim 21:

Boneh discusses the information retention policy is time-based such that the set of information is purged after a certain period of time (col.5, lines 13-30).

As per claim 22:

Boneh discusses the retention policy is time-based such that the set of information is purged when one or more conditions are satisfied (col.6, lines 6-15).

As per claim 23:

Boneh, Et Al. teaches a method for managing information retention system (col.5, lines 63-67) wherein includes a central file server 102 having a number of files of electronic information and encrypts the key file before the key file is transferred to the backup system (col.4, lines 17-21).

Boneh discloses the server system receiving a set of information and associating one or more keys with the set of information wherein encrypting the set of information using one or more keys (col.4, lines 53-55). Boneh discusses

the set of information is encrypted and storing it in the information system in the form of a backup system (col.4, lines 50-53) and the backup system provides persistent storage for only encrypted information wherein it is inherent the backup system only stores the encrypted information since the information needed to be encrypted before transferring the file to the backup system (col.4, lines 38-42). Hence, the unencrypted set of information is not persistently stored in the backup system.

In addition, Boneh discloses purging the set of information from the system by deleting the key once the key's lifetime is expired or considered as old keys thereby making the set of information inaccessible or unrenderable to a user (col.5, lines 13-22). To purge is to eliminate and to render to produce an image from the data file so unrenderable is to unable to produce the image from the data file. The information set disclosed in Boneh that is associated to the key is unable to be produced or accessed from the system once the key of that particular file is deleted (col.4, line 65 thru col.5, line 12). Thus, the set of information is inherently no longer available within the system once the key to that particular information set is deleted.

As per claim 24:

Boneh teaches the set of information is purged from the system without requiring that the encrypted form of the set of information be deleted from the one or more repositories (col.5, lines 1-32).

As per claim 25:

Boneh discloses the set of information is stored in the one or more repositories only in encrypted form (col.4, lines 50-55).

As per claim 26:

Boneh includes the keys comprises a symmetrically paired set of keys (col.7, lines 45-62).

As per claim 27:

Boneh discloses having instructions (col.5, lines 13-27) for causing the processor(s) to receive a request from an information sink to render the set of information to a user prior to deletion of one or more keys (col.6, lines 26-50). The information sink is a device that receives information from another device. Boneh teaches an information sink involving a network server such as the Internet server and a computer system for communicating information over a network (col.7, lines 28-62). Boneh further includes instructions for causing the processor(s) to access the encrypted set of information from one or more of the repositories, decrypting the encrypted set of information using a key to derive the set of information (col.7, lines 49-51), and enabling the information sink to render the set of information to the user (col.7, lines 28-62).

As per claim 28:

Boneh discloses the set of information is stored in the one or more repositories only in encrypted form (col.4, lines 50-55) and the encrypted information set is

decrypted only when it is necessary to render the set of information to the user (col.8, lines 18-28).

As per claim 29:

Boneh discloses having instructions for causing the processor(s) to receive a request from an information sink to render the set of information to a user prior to deletion of one or more keys (col.6, lines 26-50). The information sink is a device that receives information from another device. Boneh teaches an information sink involving a network server such as the Internet server and a computer system for communicating information over a network (col.7, lines 28-62). Boneh further includes instructions for accessing the encrypted set of information from one or more of the repositories, accessing one or more keys (col.4, lines 50-55), and providing the encrypted information and key(s) to enable the information sink to decrypt the encrypted set of information using the key(s) to render the set of information to the user (col.7, lines 28-62).

As per claim 30:

Boneh discloses the set of information is stored in the one or more repositories only in encrypted form (col.4, lines 50-55) and the encrypted information set is decrypted by the information sink only when it is necessary to render the set of information to the user (col.8, lines 18-28). See also col.7, lines 45-62.

As per claim 31:

Boneh discloses determining the method of purging based upon an information retention policy (col.5, lines 25-31), whether the set of information should be

purged from the system and should the information set determined to be purged wherein Boneh teaches purging the set of information by deleting the key(s) (col.6, lines 13-15). Thus, making the set of information unrenderable (col.6, lines 13-15).

As per claim 32:

Boneh discusses the information retention policy is time-based such that the set of information is purged after a certain period of time (col.5, lines 13-30).

As per claim 33:

Boneh discusses the retention policy is time-based such that the set of information is purged when one or more conditions are satisfied (col.6, lines 6-15).

Reexamination Remarks

The Examiner maintains the rejection with the prior art of Boneh wherein Boneh teaches the claim language of the amended claims 1, 12, and 23. Boneh teaches the system associating the keys with the set of information and encrypting it before storing the encrypted information and not the unencrypted form to the backup system (col.4, lines 38 thru col.5, line 5). Applicant's "information system" is the backup system of Boneh where it is inherent the backup system only stores the encrypted information since the

information needed to be encrypted by the encryption device prior to storing the file within the backup system (col.4, lines 17-44). Hence, Boneh does not leave any "local persistent file" unencrypted within the backup system. In addition, Boneh teaches that once the key file is lost or deleted, the set of information is inaccessible (col.5, lines 1-5).

Applicant claims that the information is being purged by deleting the keys. To purge is to eliminate and to render to produce an image from the data file so unrenderable is to unable to produce the image from the data file. Thus, the data associated to the key is unable to be produced or accessed from the system once the key of that particular file is deleted. Further, claims 1, 12, and 23 discloses new matter of having the set of information not being available within the system. Specification, on page 10, discusses purging the set of information wherein making the information unrenderable to the user. Specification states that "it is not necessary to delete an information set from a system in order to purge it" (lines 11-13) and also states "that it is effectively purged from the system even if it remains physically within the system" (lines 15-16). Hence, the "information is not available within the system" seems to convey (of the specification) the information sets are still within the system but just unrenderable to the user.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100